

7.0 SPACECRAFT SAFETY ASSESSMENT

7.1 RESPONSIBILITY & SCOPE

It is the responsibility of the WIRE spacecraft project organization to provide for the safety of their systems and verify compliance with applicable requirements. The following assessment to addresses identified hazards, and the actions taken to eliminate or control these hazards to meet EWR 127-1 requirements.

7.2 SYSTEM SAFETY PROGRAM

The WIRE payload organization has established and is maintaining a system safety program to support efficient and effective achievement of overall NASA system safety objectives.

7.2.1 System Safety Objectives

The WIRE payload organization has established a comprehensive system safety plan. The system safety plan has defined a systematic approach to assure that:

- A. Safety, consistent with mission requirements, is designed into the system in a timely, cost-effective manner.
- B. Hazards associated with each system are identified, tracked, evaluated, and eliminated, or the associated risk reduced to a level acceptable throughout the system life cycle.
- C. Historical safety data, including lessons learned from other systems, are considered and used.
- D. Minimum risk is sought in accepting and using new technology, materials or designs; and new production, test and operational techniques.
- E. Actions taken to eliminate hazards or reduce risk to an acceptable level are documented in the Payload Hazard Reports.
- F. Changes in design, configuration, or mission requirements are accomplished in a manner that maintains an acceptable risk level.
- G. Consideration is given early in the design and planning phase to safety and ease of disposal of any hazardous materials associated with the system. Actions will be taken to minimize the use of hazardous materials and, therefore, minimize the risks and payload design, planning, and mission costs associated with their use.

7.2.2 System Safety Requirements/Guidelines

Pertinent NASA standards, specifications, regulations, design handbooks, safety design checklists, and other sources of design guidance were reviewed for applicability. System safety design requirements were then specified.

The following general system safety guidelines were followed:

- a. Eliminate identified hazards or reduce associated risk through design, including material selection or substitution. When potentially hazardous materials must be used, select those with least risk throughout the different phase of the WIRE payload.
- b. Isolate hazardous substances, components, and operations from other activities, areas, personnel, and incompatible materials.
- c. Locate equipment so that access during operations, servicing, maintenance, repair, or adjustment minimizes personnel exposure to hazards (e.g., hazardous chemicals, high voltage, electromagnetic radiation, sharp edges or points).
- d. Minimize risk resulting from excessive environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration and vibration).
- e. Design to minimize risk created by human error in the operation and support of the system.
- f. Consider alternative approaches to minimize risk from hazards that cannot be eliminated by design. Such approaches include interlocks, redundancy, fail safe design, system protection, fire suppression, and protective clothing, equipment, devices, and procedures.
- g. Protect the power sources, controls and critical components of redundant subsystems by physical separation or shielding.
- h. When alternative design approaches cannot eliminate the hazard, provide safety and warning devices and warning and caution signs in assembly, operations, maintenance and repair instructions, and distinctive markings on hazardous components and materials, equipment, and facilities to ensure personnel and equipment protection.
- i. Minimize the severity of personnel injury or damage to equipment in the event of a mishap.
- j. Design software controls or monitor functions to minimize initiation of hazardous events or mishaps.

7.3 PRELIMINARY HAZARD ANALYSIS

A Preliminary Hazard Analysis (PHA) was done concurrent with the Systems Design Review. Identified hazards were documented and recommended actions were made for their elimination or control during the system acquisition cycle. These hazards were assessed against prior SMEX missions for similarity.

7.4 RISK ASSESSMENT

Hazard resolution methodologies are based on assessment of the risk involved. To aid the hazard elimination and control process, hazards have been ranked in terms of hazard severity and hazard probability levels. The hazard probability and hazard severity is used to establish priorities for corrective action and resolution of identified hazards. The hazard identification and elimination or control process is documented in NHB 1700.1, NASA Safety Policy and Requirements Document. Detailed review of this document and the attached Payload Hazard Reports will assist in the overall elimination and control of risk.

7.4.1 Hazard Severity

Hazard severity categories, shown in Table 7-1 are defined to provide a qualitative measure of the worst credible mishap resulting from personnel error; environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem or component failure or malfunction.

Table 7-1 Hazard Severity

Description	Category	Definition
CATASTROPHIC	I	Death, system loss, or severe environmental damage.
CRITICAL	II	Severe injury, severe occupational illness, major system or environmental damage.
MARGINAL	III	Minor injury, minor occupational illness, or minor system or environmental damage.
NEGLIGIBLE	IV	Less than minor injury, occupational illness, or less than minor system or environmental damage.

NHB 1700.1 (VI-B)

7.4.2 Hazard Probability

The probability that a hazard will occur during the life expectancy of the system can be described in potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Hazard probability ranking is shown at Table 7-2.

Table 7-2 HAZARD PROBABILITY LEVELS

LEVEL	FREQUENCY OF OCCURENCE	DEFINITION
A	Frequent	Likely to occur one or more times during the life of the WIRE program
B	Reasonably probable	Likely to occur several times during the life of the WIRE program
C	Occasional	Likely to occur sometime during the life of the WIRE program
D	Remote	Unlikely, but possible to occur in the life of WIRE
E	Improbable	So unlikely, it can be assumed occurrence may not be experienced

NHB 1700.1 (VI-B)

7.4.3





Hazard Risk Assessment Matrix

The Hazard Risk Index (HRI) is a number derived by considering both the severity and the probability of a hazard, as shown in Table 7-3. The HRI presents hazard analysis data in a format that helps the managing activity make decisions regarding whether hazards should be eliminated, controlled, or accepted. The HRI provides the basis for logical management decision making by considering both the severity and probability of a hazard. It should be noted that, for valid risk assessment, the potential severity of a hazard may not decreased unless physical changes are made to completely eliminate the hazards. The probability can be greatly reduced by design modifications, or by incorporating safety devices, warning devices, or special procedures thereby reducing the HRI.

Table 7-3 RISK MATRIX

Frequency of Occurrence	Hazard Categories			
	I Catastrophic	II Critical	III Marginal	IV Negligible
(A) Frequent	1A	2A	3A	4A
(B) Probable	1B	2B	3B	4B
(C) Occasional	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Improbable	1E	2E	3E	4E

NHB 1700.1 (VI-B)

<u>Hazard Risk Index</u>		<u>HRI</u>	<u>Suggested Criteria</u>
1A, 1B, 1C, 2A, 2B, 3A		1	Unacceptable
1D, 2C, 2D, 3B, 3C		2	Undesirable (Management Decision Required)
1E, 2E, 3D, 3E, 4A, 4B		3	Acceptable with review by Management
4C, 4D, 4E		4	Acceptable without review

7.5 HAZARDS RESOLUTION & TRACKING

The WIRE payload organization goal is to eliminate identified hazards or reduce the associated risk to a level defined by or acceptable to the Western Range. Resolution of catastrophic and critical hazards will not rely solely on warnings, cautions or procedures/training for control of risk. Hazards documented in the Payload Hazard Reports and will be updated, reviewed, and approved during the phased safety review process established in EWR 127-1.

7.6 SAFETY ASSESSMENT SUMMARY

The safety assessment data in this document is provided to meet the requirements of EWR 127-1.

7.6.1 Safety Requirements Compliance Summary

The WIRE payload is in compliance with all applicable requirements of EWR 127-1.

7.6.2 Equipment and Facility Assessment

The following subsections address the major safety issues related to the WIRE payload and facility operations.

7.6.2.1 Ground Support Equipment and Facilities

A description of the GSE and facilities to be used is provided in Section 4.0. All of the equipment and the required facility support/interfaces associated with WIRE are in compliance with appropriate requirements and criteria.

7.6.2.2 Material Handling Equipment

The material handling equipment associated with WIRE is described in Section 4.1.1. Hardware and special lifting fixtures used to handle critical equipment will be retested to 200% of their rated load annually or within 12 months prior to use. Note that lifting equipment used to handle critical loads will receive annual capability verification. Equipment used to handle non-critical loads will be tested every four years.

All technical personnel involved with WIRE assembly will be trained and certified prior to performing processes at the range. Detailed lifting procedures will define the assembly, handling, and transportation operations.

7.6.2.3 Noise Protection

Currently no equipment, procedures, or operations associated with or related to WIRE have been identified that exceed 85 dBA.

7.6.2.4 Non-Ionizing Radiation

The WIRE spacecraft has a transponder/two antenna that are identified as potential non-ionizing radiation sources. Details regarding these devices is provided in Section 3.2.6.2

7.6.2.5 Ionizing Radiation

There are no ionizing radiation sources associated with the WIRE spacecraft or support equipment.

7.6.2.6 Hazardous Materials

Descriptions of the hazardous materials associated with the WIRE spacecraft and ground processing activities are provided in Sections 3.10.1, 3.2.10, and 4.8. MSDS's are located in Appendix B.

7.6.2.7 Propellants and Systems

The WIRE spacecraft has no propellant or propulsion system.

7.6.2.8 Pressurized Systems

Three steps have been taken to assure the safety of personnel and equipment associated with WIRE operations, due to the hazards associated with pressurized H₂. First, the cryostat is designed to pressure-vessel codes. Second, redundant burst disks are provided to vent the H₂ if it reaches a higher-than-normal pressure; and third, the burst disk vents are manifolded together and exhaust into a common safety vent line that exits to the atmosphere where H₂ can be safely dissipated.

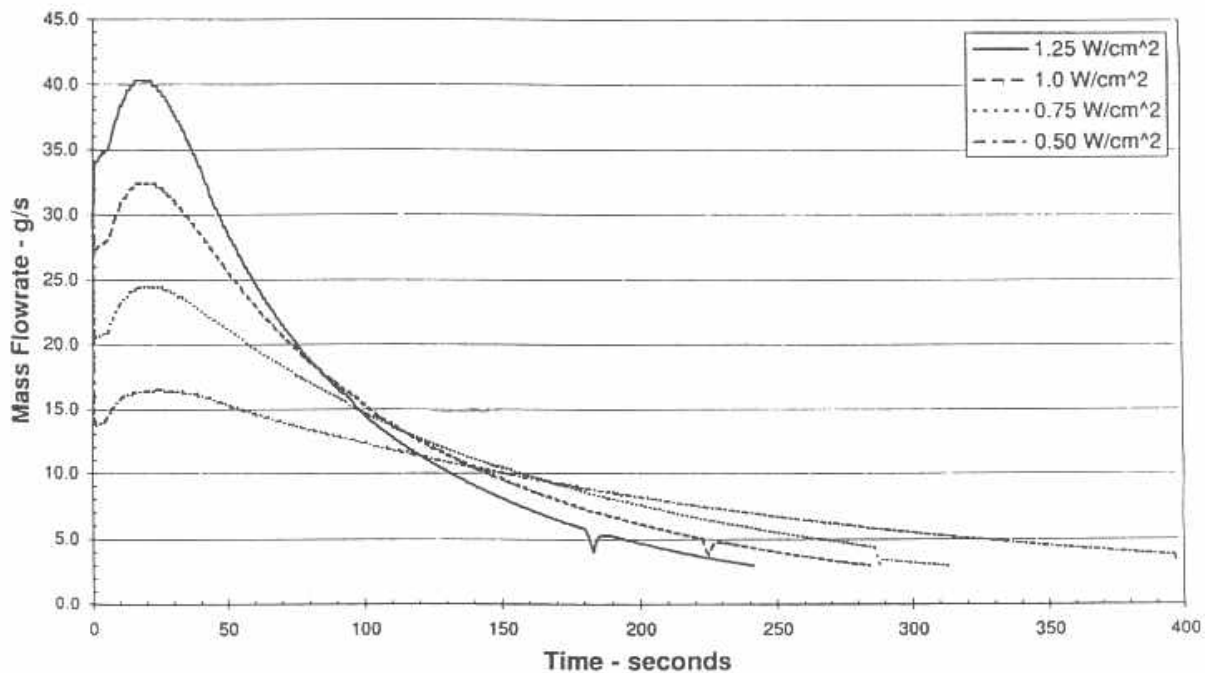
7.6.2.8.1 Design factors of safety

The vacuum shell and H₂ tanks are designed to meet MIL-STD-1522A, Section 5, Approach C, which specifies the pressure code requirement called for in the 1983 ASME Boiler and Pressure Vessel Code, Section 8, "Rules for Construction of Pressure Vessels, Division 1." The ASME Boiler Code requires a factor of safety of four times the MEOP for internal pressure differentials and two times MEOP for external pressure differentials.

Because the WIRE vacuum shell and primary and secondary tanks will nominally operate at negative pressures, MEOP criteria do not apply. LMMS has instead designed these vessels and external plumbing to meet a factor of safety of four times the MDP for internal pressure differentials and two times MDP for external differentials. The primary and secondary tanks and the plumbing inside the vacuum have been designed for an MDP of 40 psi internally and an MDP of 15 psi externally. The primary vent valve and the rest of the external plumbing, however, has been designed to meet a MDP of 30 psi internally and a MDP of 15 psi externally. The vacuum shell has been designed to meet a MDP of nine psid internally a MDP of 15 psid externally.

The H₂ tanks (both primary and secondary) are designed with a MDP of 40 psi for the worst possible failure scenario because of the risks associated with handling and ground filling operations. The worst-case heat load condition (Figure 7-1) for the cryostat is a rapid loss of vacuum that introduces unlimited ambient air into the vacuum insulated space. In this scenario, the warm air condenses on the H₂-filled tanks, placing a large load on the cryogen and causing it to expand rapidly. The ensuing pressure rise inside the tanks ruptures the burst disks, and H₂ gas vents.

**Figure 7-1 Safety Vent H₂ Flow Rate History:
Catastrophic Loss of Vacuum (1.25 W/cm²) and Lower Heat Rate Reference Cases**

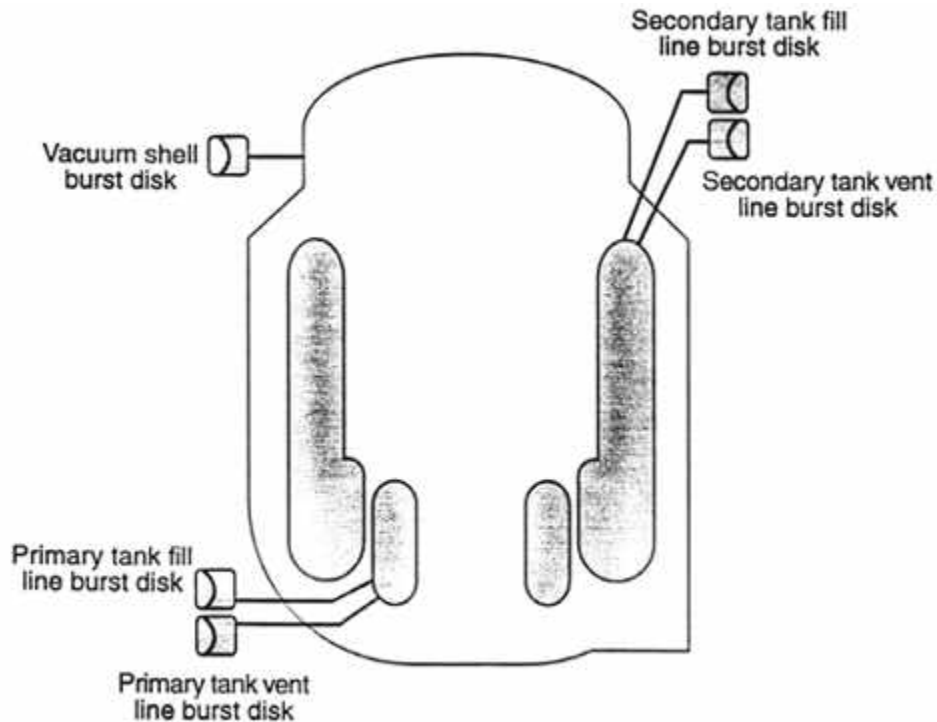


This is not a failure scenario that would occur as a result of leaking O-rings or even a small weld leak. This failure calls for the “remote” possibility of a handling accident during which pieces of equipment (tools, forklift) puncture the external vacuum shell, resulting in hole the order of one-half inch in diameter or larger. The analysis for this case has been used for previous LMMS cryostat designs including CLAES and SPIRIT III, and shows a peak flow rate of 40 g/s, lasting less than a minute. All liquid is gone under three minutes. The average flow rate is 25 g/s.

7.6.2.8.2 Burst disks

The WIRE cryostat system is protected from overpressure by five burst disks located in the vacuum shell, the primary tank fill line, the primary tank vent line, the secondary tank fill line, and the secondary tank vent line. The manifolded safety vent and burst disk locations on the H₂ tanks and vacuum shell is shown in Figure 7-2. If a burst disk on the orbit vent line fails, preventing gas from reaching and venting through the safety vent line, the burst disk on the fill line would rupture, allowing the gas to vent through the safety vent. Note that a burst disk rupture on a tank would occur only if the pressure within it exceeded $15 \pm$ psi above the external pressure; likewise, a burst disk rupture on the vacuum shell would occur only if the pressure within it exceeded 9 ± 1 psid. These pressure are well below the pressure capabilities of the cryostat.

**Figure 7-2 Manifolded Safety Vent and Burst Disk Locations
on H₂ Tanks and Vacuum Shell**



7.6.2.8.3 Common safety vent line

The five burst disks are manifolded together into a common safety vent line. (See to Figure 7-2). Because the burst disk pressures are much lower than the pressure capability of the H₂ tanks, vacuum shell, and the external plumbing, venting can take place only through this safety vent line, which safely exhausts to the ground-based or airborne safety vent system. While the instrument is in the PPF, during the H₂ fill and Pegasus fairing installation, the safety vent line is connected to a facility vent stack that vents to the atmosphere. A GSE check valve is installed on the safety vent at the exit from the cryostat and GHe will be used to purge the safety vent line between the outlet of each burst disk and the check valve. This prevents air from entering the cryostat if a burst disk happens to rupture during a time when the building vent is not being purged or is not connected. Once the cryostat is connected to the OSC vent line through the Pegasus, the check valve will be removed and the He purge must then be maintained. The facility vent stack is purged with GHe to maintain an inert atmosphere in the vent line and stack at all times (SPIRIT III used a flow rate of 35 cu ft/hr to maintain the inert atmosphere).

During transportation to the hot pad, a “portable” vent stack will be used. This same portable stack will also be used during Pegasus mating to the L-1011 and any hot pad operations. This safety vent line connects to an OSC provided vent interface to vent any H₂ that is escaping the launch vehicle away from the carrier aircraft. During flight operations, such as rollout and

taxiing, captive carry, and any abort scenarios, the safety vent line exits the launch vehicle fairing directly to the outdoors. Again, the safety vent will be purged with GHe.

Table 7-4 shows the pressure capabilities for the cryostat vacuum shell, H₂ tanks and plumbing, the primary vent, and the safety vent. Table 7-5 provided pertinent fabrication information on the cryostat vacuum shell.

Table 7-4 WIRE Cryostat Pressure Capability
(differential pressures in psi)

	Primary Tank (& Plumbing)	Primary Vent Line	Secondary Tank (& Plumbing)	Vacu m Shell	External Plumbing	Safety Vent
MDP internal	40	30	40	9	15	5
MDP external	15	15	15	15	15	15
Design internal	160	120	160	36	60	20
Design external	30	30	30	30	30	30
Test internal (1.5 MDP internal)	60	45	60	14	22	TBD
Maximum burst disk rupture	15 (±1)	15 (±1)	15 (±1)	9 (±1)	9 (±1) -15 (±1)	NA
Maximum reverse pressure change	30	30	30	30	30	NA

Table 7-5 WIRE Cryostat Vacuum Shell Data

Pressurant/Volume	Vacuum, -244 liters
Dimensions	Outer dimensions of WIRE: 26-in. wide x38-in. high
Construction materials	6061-T6 Al ring-stiffened cylinder and domed shells, epoxy-bonded rear dome and front conical sections
MDP @ nominal temperatures	9 psi
Maximum allowable working pressure	0 psia
MDP (after 1 failure)	9 psid
Proof pressure	14 psi
Shell design pressure (internal)	36 psid
Actual burst disk pressure	9 psid

7.6.2.9 Ordnance Systems

The WIRE instrument ordnance activation has a minimum of three inhibits. Details regarding the ordnance system are provided in Section 3.1.5.1

7.6.2.10 Electrical and Electronic Systems

Electrical faults in the WIRE spacecraft and instrument EGSE are addressed in the appropriate Payload Hazard Reports. Fusing and wiring data is provided in Appendix C.

7.6.2.11 Computing Systems and Software

A description of the computing systems and software associated with WIRE and its support equipment are provided in Section 3.2.11.

7.7 PAYLOAD HAZARD REPORTS

Safety concerns and hazards were identified during the preliminary hazard analysis and the initial risk assessment process major. The following Hazard Reports, included as Appendices D and E, address all identified catastrophic and critical hazards that require review and approval by the Western Range.

Spacecraft Hazard Reports:

WIRE-1	Structural Failure of Flight Hardware
WIRE-2	Structural Failure of WIRE Mechanical Ground Support Equipment
WIRE-3	Ground Handling Operational Error
WIRE-4	Structural Failure of WIRE Battery
WIRE-5	Electrical Failure of WIRE Battery
WIRE-6	Electrical Failure or Improper Operation of Battery EGSE
WIRE-7	Electrical Fault in Spacecraft and Instrument EGSE
WIRE-8	Exposure to Non-ionizing Radiation.
WIRE-9	EGSE or MGSE Equipment Moves, Falls, or is Upset

Instrument Hazard Reports: